CLAIMS

1. A computer system, comprising:

a data-handling system operable to receive and transmit data over a data path;

a storage device operatively coupled to the data-handling system to receive data from and deliver stored data to the data-handling system; and

a security element operatively coupled between an external data path and the data-handling system via the data path, the security element establishing the data path as a trusted path,

wherein the data-handling system, the storage device and the security element are disposed in a common physical housing such that access to the data path requires breach of the housing.

2. The computer system of claim 1, wherein the data-handling system includes one or more servers, client terminals, and/or databases.

3. The computer system of claim 1, wherein the security element is one of a hardware solution and a software solution.

(VPN) to shield one or more servers (e.g., banks of servers or individual servers). Intrusion Detection Systems (IDSs)

4. The computer system of claim 1, wherein the security device is operable to establish at least one of (i) a firewall function, (ii) a virtual private network function, (iii) an intrusion detection system function, (iv) a virus screen function, (v) a URL filter function, (vi) a spam filter function, and (vii) a fire door function.

5. A computer system, comprising:

a data-handling system operable to receive and transmit data over a data path;

a storage device operatively coupled to the data-handling system to receive data from and deliver stored data to the data-handling system; and

a security element operatively coupled between an external data path and the data-handling system via the data path, the security element establishing the data path as a trusted path,

wherein the security element is disposed in a separate physical housing from the data-handling system and the storage device, and the data path is encased in an armored sheath operable to substantially resist access to the data path by unauthorized entities.

6. The computer system of claim 5, further comprising one or more anti-tamper devices integrated with one or more connectors of the data path, the anti-tamper devices resisting removal of the one or more connectors from at least one of the data-handling system and the security device.

7. The computer system of claim 6, wherein the anti-tamper devices are operable to permanently damage at least one of themselves and mating connectors thereof in order to substantially resist access to the data path by unauthorized entities.

8. The computer system of claim 6, wherein the anti-tamper devices include at least one barb that interlocks with a mating element of a mating connector such that the connector may not be removed from the mating connector without damaging at least one of the connector and mating connector in order to substantially resist access to the data path by unauthorized entities.

9. The computer system of claim 8, wherein:

the at least one barb is formed from a flexible yet sturdy metal that is biased in an outward direction away from the connector; and

the mating connector includes one or more corresponding ridges, channels, and/or protrusions that engage the at least one barb to fixedly couple the connector and the mating connector together.

10. The computer system of claim 5, further comprising an intelligent device coupled along the data path that is operable to detect a decoupling of the security element from the data-handling system and to take action in response.

11. The computer system of claim 10, wherein the intelligent device is operable to sound an alarm when decoupling of the security element from the data-handling system is detected.

12. The computer system of claim 10, wherein the alarm may be directed to a specific network address.

13. The computer system of claim 10, wherein the intelligent device is operable to record that decoupling of the security element from the data-handling system is detected.

14. The computer system of claim 10, wherein the intelligent device is operable to sense a lack of current to receiving drivers in either the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

15. The computer system of claim 10, wherein the intelligent device is operable to open the data path between the data-handling device and the security element in response to a decoupling of the security element from the data-handling system.

16. The computer system of claim 15, wherein the intelligent device is operable to open a fusible circuit in response to the decoupling of the security element from the data-handling system.

17. The computer system of claim 10, wherein the intelligent device is operable to sense a lack of response to an initiated ping signal to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

18. The computer system of claim 10, wherein the intelligent device is operable to sense unpredicted responses to a systematic sequence of initiated ping signals to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

19. The computer system of claim 5, wherein the data-handling system includes one or more servers, client terminals, and/or databases.

20. The computer system of claim 5, wherein the security element is one of a hardware solution and a software solution.

21. The computer system of claim 5, wherein the security device is operable to establish at least one of (i) a firewall function, (ii) a virtual private network function, (iii) an intrusion detection system function, (iv) a virus screen function, (v) a URL filter function, (vi) a spam filter function, and (vii) a fire door function.

22. A security element operatively connectable between an external data path and a data-handling system via a data path, wherein: (i) the security element establishes the data path as a trusted path, (ii) the security element is disposed in a separate physical housing from the data-handling system and an associated storage device, and (iii) the data path is encased in an armored sheath operable to substantially resist access to the data path by unauthorized entities.

23. The computer system of claim 22, further comprising one or more anti-tamper devices integrated with one or more connectors of the data path, the anti-tamper devices resisting removal of the one or more connectors from at least one of the data-handling system and the security device.

24. The computer system of claim 23, wherein the anti-tamper devices are operable to permanently damage at least one of themselves and mating connectors thereof in order to substantially resist access to the data path by unauthorized entities.

25. The computer system of claim 23, wherein the anti-tamper devices include at least one barb that interlocks with a mating element of a mating connector such that the connector may not be removed from the mating connector without damaging at least one of the connector and mating connector in order to substantially resist access to the data path by unauthorized entities.

26. The computer system of claim 25, wherein:

the at least one barb is formed from a flexible yet sturdy metal that is biased in an outward direction away from the connector; and

the mating connector includes one or more corresponding ridges, channels, and/or protrusions that engage the at least one barb to fixedly couple the connector and the mating connector together.

27. The computer system of claim 22, further comprising an intelligent device coupled along the data path that is operable to detect a decoupling of the security element from the data-handling system and to take action in response.

28. The computer system of claim 27, wherein the intelligent device is operable to sound an alarm when decoupling of the security element from the data-handling system is detected.

29. The computer system of claim 27, wherein the alarm may be directed to a specific network address.

30. The computer system of claim 27, wherein the intelligent device is operable to record that decoupling of the security element from the data-handling system is detected.

31. The computer system of claim 27, wherein the intelligent device is operable to sense a lack of current to receiving drivers in either the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

32. The computer system of claim 27, wherein the intelligent device is operable to open the data path between the data-handling device and the security element in response to a decoupling of the security element from the data-handling system.

33. The computer system of claim 32, wherein the intelligent device is operable to open a fusible circuit in response to the decoupling of the security element from the data-handling system.

34. The computer system of claim 27, wherein the intelligent device is operable to sense a lack of response to an initiated ping signal to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

35. The computer system of claim 27, wherein the intelligent device is operable to sense unpredicted responses to a systematic sequence of initiated ping signals to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

36. The computer system of claim 22, wherein the security element is one of a hardware solution and a software solution.

37. The computer system of claim 22, wherein the security device is operable to establish at least one of (i) a firewall function, (ii) a virtual private network function, (iii) an intrusion detection system function, (iv) a virus screen function, (v) a URL filter function, (vi) a spam filter function, and (vii) a fire door function.

38. A security cable operatively connectable between a security element and a data-handling system to establish a data path therebetween, wherein: (i) the security element establishes the data path as a trusted path, (ii) the security element is disposed in a separate physical housing from the data-handling system and an associated storage device, and (iii) the data path is encased in an armored sheath operable to substantially resist access to the data path by unauthorized entities.

39. The security cable of claim 38, further comprising one or more anti-tamper devices integrated with one or more connectors of the data path, the anti-tamper devices resisting removal of the one or more connectors from at least one of the data-handling system and the security device.

40. The security cable of claim 39, wherein the anti-tamper devices are operable to permanently damage at least one of themselves and mating connectors thereof in order to substantially resist access to the data path by unauthorized entities.

41. The security cable of claim 39, wherein the anti-tamper devices include at least one barb that interlocks with a mating element of a mating connector such that the connector may not be removed from the mating connector without damaging at least one of the connector and mating connector in order to substantially resist access to the data path by unauthorized entities.

42. The security cable of claim 41, wherein:

the at least one barb is formed from a flexible yet sturdy metal that is biased in an outward direction away from the connector; and

the mating connector includes one or more corresponding ridges, channels, and/or protrusions that engage the at least one barb to fixedly couple the connector and the mating connector together.

43. The security cable of claim 38, further comprising an intelligent device coupled along the data path that is operable to detect a decoupling of the security element from the data-handling system and to take action in response.

44. The security cable of claim 43, wherein the intelligent device is operable to sound an alarm when decoupling of the security element from the data-handling system is detected.

45. The security cable of claim 43, wherein the alarm may be directed to a specific network address.

46. The security cable of claim 43, wherein the intelligent device is operable to record that decoupling of the security element from the data-handling system is detected.

47. The security cable of claim 43, wherein the intelligent device is operable to sense a lack of current to receiving drivers in either the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

48. The security cable of claim 43, wherein the intelligent device is operable to open the data path between the data-handling device and the security element in response to a decoupling of the security element from the data-handling system.

49. The security cable of claim 48, wherein the intelligent device is operable to open a fusible circuit in response to the decoupling of the security element from the data-handling system.

50. The security cable of claim 43, wherein the intelligent device is operable to sense a lack of response to an initiated ping signal to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

51. The security cable of claim 43, wherein the intelligent device is operable to sense unpredicted responses to a systematic sequence of initiated ping signals to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

52. A computer system, comprising:

a data-handling system operable to receive and transmit data over a first data path;

a storage device operatively coupled to the data-handling system via a second data path to receive data from and deliver stored data to the data-handling system; and

a security element operatively coupled between an external data path and the data-handling system via the data path, the security element establishing the data path as a trusted path,

wherein at least one of the data-handling system, the storage device, and the security element is disposed in a separate physical housing from the other elements of the

system, and one or more of the data paths are encased in an armored sheath operable to substantially resist access to the data path by unauthorized entities.

53. The computer system of claim 52, further comprising one or more anti-tamper devices integrated with one or more connectors of the data path, the anti-tamper devices resisting removal of the one or more connectors from at least one of the data-handling system and the security device.

54. The computer system of claim 53, wherein the anti-tamper devices are operable to permanently damage at least one of themselves and mating connectors thereof in order to substantially resist access to the data path by unauthorized entities.

55. The computer system of claim 53, wherein the anti-tamper devices include at least one barb that interlocks with a mating element of a mating connector such that the connector may not be removed from the mating connector without damaging at least one of the connector and mating connector in order to substantially resist access to the data path by unauthorized entities.

56. The computer system of claim 55, wherein:

the at least one barb is formed from a flexible yet sturdy metal that is biased in an outward direction away from the connector; and

the mating connector includes one or more corresponding ridges, channels, and/or protrusions that engage the at least one barb to fixedly couple the connector and the mating connector together.

57. The computer system of claim 52, further comprising an intelligent device coupled along the data path that is operable to detect a decoupling of the security element from the data-handling system and to take action in response.

58. The computer system of claim 57, wherein the intelligent device is operable to sound an alarm when decoupling of the security element from the data-handling system is detected.

59. The computer system of claim 57, wherein the alarm may be directed to a specific network address.

60. The computer system of claim 57, wherein the intelligent device is operable to record that decoupling of the security element from the data-handling system is detected.

61. The computer system of claim 57, wherein the intelligent device is operable to sense a lack of current to receiving drivers in either the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

62. The computer system of claim 57, wherein the intelligent device is operable to open the data path between the data-handling device and the security element in response to a decoupling of the security element from the data-handling system.

63. The computer system of claim 57, wherein the intelligent device is operable to open a fusible circuit in response to the decoupling of the security element from the data-handling system.

64. The computer system of claim 57, wherein the intelligent device is operable to sense a lack of response to an initiated ping signal to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.

65. The computer system of claim 57, wherein the intelligent device is operable to sense unpredicted responses to a systematic sequence of initiated ping signals to at least one of the data-handling device or the security element in order to detect a decoupling of the security element from the data-handling system.